A new object in the sky

Space law points the telescope to its relationship with cyber law

---

ajv2016 2019-01-30T09:41:42

While cyber activities have been growing rapidly since the 1970's, the law was not able to catch up with this development immediately. However, over the years, law-making efforts at the international level have resulted in the enactment of international conventions regarding cybercrime such as the United Nations Convention Against Transnational Organized Crime, the Budapest Convention on Cyber Crime, or the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Yet, international law on cyberspace is still underdeveloped: Beyond the area of cybercrime international legal instruments are largely lacking. Hence, the question comes up if other similar regimes of international law could provide normative guidelines for cyberspace and cyber activities. This post aims to highlight that an international legal discourse on the relationship between space law and cyber law is emerging and that this discourse may provide important insights for the development of international cyber norms.

The Emerging Discourse on the Interrelation between Space Law and Cyber Law

As is known, after Estonian e-services, both public and private, were subject to malicious cyber-attacks in 2007, NATO took the initiative to establish the Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in that country in 2008. The Centre has invited scholars and practitioners, working on different legal regimes, to prepare a guidebook for States to address the applicability of international law and its specific branches to cyber activities.

The Centre's activities led to the first guidelines on the subject, entitled *"Tallinn Manual on the International Law Applicable to Cyber Warfare"* in 2013. In this first edition, which addressed especially the applicability of international law to cyber warfare, there had been no mention of the relationship between space law and cyber activities. However, a new volume with an expanded scope was released in 2017 by Cambridge University Press, titled *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations",* and the guidelines in the Manual were put together with the specific aim to embrace broader matters regarding cyber activities, including the implementation of space law to cyber space in some cases.

Apart from the work of the NATO CCD COE, the relationship between space law and cyber law has drawn the attention of several space law researchers such as *Stephan Hobe, Stefan A. Kaiser,* and *Martha Mejía-Kaiser*. The International Institute of Space Law (IISL), has started to look closer at the relationship between space and cyber activities, and examined how space law could be applied to cyber activities.

The IISL has embarked on the topic through the establishment of the Working Group on Cyber Law chaired by Stephan Hobe, and the group concluded its final report in August 2017.

In the report, the working group demonstrated the connection between these two activities, suggested that especially the terminology of the cyber activities should be clarified, and that clarification could be achieved through the interpretation of existing space law terminology and concepts. Therefore, it was recommended by the Working Group to the Institute's Board of Directors to add cyber law as a topic for future IISL Colloquia. In this way, this year's IISL Colloquium on the Law of the Outer Space, at the 69th International Astronautical Congress (IAC) (held 1-5 October 2018), for the first time included a session titled "*The Relationship Between Space Law and Cyber Law, and Other Recent Developments in Space Law*". Henceforward, the topic has surfaced on the agenda of the space law community.

The Application of Space Law to Cyber Activities

To dive into this topic, the application of space law to cyber activities can be examined in two categories. The first category is the application of space law to general cyber law and cyber activities by analogy. The second is the application of space law to cyber activities in outer space.

Regarding the first category, the general principles of space law may be applicable to cyberspace and cyber activities by analogy, as cyberspace and outer space – despite their obvious differences – both represent a common good of the international society and require cooperation for their protection. Several international legal scholars support the proposition to apply general space law principles to cyberspace by analogy: For instance, *Mejía-Kaiser* embraces the analogy method in her article "*Space Law and Unauthorised Cyber Activities",* in the book titled **"**Peacetime Regime for State Activities in Cyberspace International Law", to reveal which principles of space law could be applied to cyber activities. *Ziolkowski* also suggests in the chapter *"General Principles of International Law as Applicable in Cyberspace"*, in the same book, that the application of general principles by analogy is not a far-reaching resolution as general principles which are deduced from other specific regimes could be used in other situations, as they are open to concretization in other situations. To put it in another way: the general principles for other commons could be applicable in cyberspace, since cyberspace like other global commons is open to the free and peaceful use of mankind.

Regarding the second category, the Tallinn Manual 2.0 specifies activities which would be subject to space law, and defines these activities as cyber-enabled space operations. As exemplified in the Manual, the activities such as employment of telemetry, tracking, command systems for communications between ground stations and spacecraft fall within this definition (Tallinn Manual 2.0, p. 270 – 271, para. 2-3).

As for implementation of space law to cyber-enabled space operations, the Tallinn Manual 2.0 proposes that the activities may be conducted only for peaceful purposes and that they are subject to the international limitation on the use of force as set forth in Article II of the Treaty on Principles Governing the Activities of States in

the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Rule 58).

Moreover, Manual 2.0 demands to avoid interference with the peaceful space activities of other States and proposes an obligation of States to supervise cyber activities of non-governmental organizations in outer space. Cyber operations involving space objects are deemed to be subject to the responsibility and liability regime of space law (Rule 59 and 60).

Outlook

Consequently, as demonstrated above it is clear that space law has a significant and substantial role to provide applicable rules not for all cyber activities but to a certain extent for some of them. However, it should be admitted that the application of principles and rules derived from space law is not the only means regarding the legal regime of cyber activities, so in addition to regulations of cybercrime, the specific legal regime with respect to cyber activities and operations is likely to develop within years.

Cite as: Merve Erdem, “A new object in the sky: space law points the telescope to its relationship with cyber law”, *Völkerrechtsblog*, 30 January 2019.
